Frequently Asked Questions on SPS for IT Administrators

This document provides information on SPS for IT Administrators in the form of question and answers. A categorized list of questions is listed below and the answers follow the list.

List of Questions

A. Installation and General Category

What is involved in installing SPS on end-user machine?

How does SPS run?

Does SPS need any maintenance-type work?

What kind network access is needed for SPS?

Why do we need a machine setup with dial-up access for SPS?

Can SPS be accessed from a different browser other than Internet Explorer?

Can Pop-ups be completely disabled in Internet Explorer for SPS?

What are the IP addresses for the DNS names used in SPS?

B. SmartCard/IKey/Token Related

What is a SmartCard/iKey/Token?

C. SPS and Java

Can SPS co-exist with other applications that use Java?

D. SPS and other Applications

Are there any issues with SPS and Momentum?

Are there any issues with SPS and CashLink?

Are there any issues with SPS and Oracle?

Are there any issues with SPS and CITRIX?

E. Public Key Infrastructure

What is the PKI (Public Key Infrastructure) used in SPS?

Can the SPS co-exist with other PKI applications?

Can SPS use/work with a different PKI?

Can SPS share credentials with other applications?

Can SPS use a different smart card/IKey?

Why does SPS not use the secure port access (636) to LDAP?

F. Security

What kind of encryption is used in SPS? What kind of security is used in SPS?

Are there any issues with SPS and NIST security recommendations?

Questions and Answers - Installation and General Category

1. What is involved in installing SPS on end-user machine?

There are five steps to install SPS: a) install SmartCard/IKey drivers, b) install Java Plug-In version 1.3.1_15, and c) install website-root SSL certificate in the Internet Explorer, d) create local directories under C:\SPS, and e) prepare Java Plug-In to accept a custom Java Applet policy file.

An installer using a Setup Factory build is used to install SPS. At the time of installation, the user logged into the end-user machine needs to have “Local Administrator” rights.

2. How does SPS run?

SPS is a “thin-client web application.” SPS is a Java Applet based application that uses a cryptographic token to securely connect and interact with back-end systems through the Internet Explorer browser. The login page of SPS is at the URL: https://sps.fms.treas.gov

When a user accesses SPS, a Java Applet is launched to run SPS code. The Java code required to run SPS is downloaded to the local machine as Java JAR files. To expedite subsequent accesses to SPS, we cache the JAR files in a local directory. To ensure that the JAR files are intact, they are cryptographically checked prior to being used.

3. Does SPS need any maintenance-type work?

No. Once SPS is installed on a machine, there is no day-to-day type maintenance work needed.

Occasionally, when newer versions of SPS are made available, the updated SPS Java Jar files are downloaded during SPS access. This happens without any special end-user or administrator intervention.

4. What kind network access is needed for SPS?

End users can either use Internet to access SPS or use dial-up telephone line to access SPS. When end users are using Internet to access SPS, the SPS application establishes a dual-authenticated and encrypted SSL connection to access backend components. How ever, since SPS is not a proxy-aware application, any intervening firewall/proxy setup needs to be configured to allow a "direct SSL" connection from end-user machines to port 443 on sps.fms.treas.gov. In addition, access to port 389 on dsa.publicdebt.treas.gov is also needed to allow SPS access LDAP service. Please note that all communication between SPS and backend components is initiated from the end-user machines.

To summarize, here is a short list of the access requirements:

1) Direct access from each client workstation to server "dsa.publicdebt.treas.gov" on TCP port 389 (LDAP).
2) Direct access from each client workstation to server "sps.fms.treas.gov" on TCP port 443 (SSL).
3) The ability to connect directly to these servers from the client workstations, without any reliance on a non-transparent web proxy server.
4) The ability to resolve the server names from the client workstations, without any reliance on a non-transparent web proxy server.

5. Why do we need a machine setup with dial-up access for SPS?

While SPS is accessed through the Internet from end-user desktops, we recommend a separate machine setup with dial-up access for contingency purposes. If your Internet connectivity is not available, or, if SPS is not available through Internet, you can still access SPS through dial-up telephone line.

6. Can SPS be accessed from a different browser other than Internet Explorer?

Even though Internet Explorer is the officially sanctioned browser for SPS, we heard from our customers that they had very good success with Netscape/Mozilla/FireFox browsers with SPS.

7. Can Pop-ups be completely disabled in Internet Explorer for SPS?

No. When SPS users select the "Help" option inside SPS, a pop-up window is opened to display help information. Disabling all pop-ups will interfere this function. You can disable pop-ups and provide an exception to SPS for pop-ups as follows: Select "Tools" menu option -> "Pop-up Blocker" -> "Pop-up Blocker Settings…" and enter "sps.fms.treas.gov" in the "Address of Website to allow:" text box. Then press "Add" button for the entry to be added to the list of the "Allowed sites" for the browser.

8. What are the IP addresses for the DNS names used in SPS?

The IP addresses for the DNS names used in SPS are made known through the usual DNS mapping mechanisms. If you can not use the DNS mapping mechanisms, you could hard-code the following IP addresses:

sps.fms.treas.gov	166.123.208.140
dsa.publicdebt.treas.gov	166.123.208.25

Please note that these addresses can change with out notice – though unlikely to happen, but not impossible.

Questions and Answers - SmartCard/IKey/Token Related

9. What is a SmartCard/iKey/Token?

Access to the SPS is controlled using the PKI (Public Key Infrastructure) credentials provided to all the end-users in the secure "Token." The credentials stored on the token is used to establish the identity of the end-user and the authorization system built-in to SPS establishes the role of the end-user. The secure token is available in two form factors: a) credit-card sized SmartCard that requires a hardware reader device attached to the end-user machine, and b) USB device that attaches directly to a USB port on the end-user machine.

Questions and Answers - SPS and Java

10. Can SPS co-exist with other applications that use Java?

Yes. The only requirement SPS has with respect to Java is this: at the time SPS needs to be accessed from the Internet Explorer browser, the Java Plug-in version 1.3.1_15 needs to be the Java Plug-in used by the browser. There can be other inactive Java Plug-in installations and there can be other Java SDK versions installed on the machine.

Questions and Answers - SPS and other Applications

11. Are there any issues with SPS and Momentum?

Momentum requires Java Plug-in version 1.4.X and during installation may force other versions of Java Plug-in versions not available for SPS. To make sure that SPS and Momentum can co-exist on the same machine, un-install Momentum and install again *without* choosing the option of Internet Explorer being the browser of choice for Momentum.

12. Are there any issues with SPS and CashLink?

CashLink requires Java Plug-in version 1.4.X and our experience has indicated that SPS and CashLink co-exist on end-user machines with out any special effort.

13. Are there any issues with SPS and Oracle?

Oracle installs one or more non-standard versions of Java with their products. We have not seen an instance where that Java version is actually used in any of their products other than during the installation process. What we have done is disabled the Java installations, and then installed SPS/ITRA.

This generally involves:

1) Un-installing any Oracle installed Java from the machine using add/remove programs
2) Renaming any Oracle installed Java folders under "C:\Program Files"
3) Deleting any Oracle installed "Java*.exe" and "Java*.dll" under C:\Windows\System32
4) Deleting any Oracle installed JavaSoft registry keys under HKLM\Software
5) Removing any Oracle installed Java references from the System and User "Path" variables in "ControlPanel-->System-->Advanced--> EnvironmentVariables"
6) Installing SPS/ITRA

Unfortunately, these steps are potentially dangerous/destructive as regards Java usage on the machine. Additionally, extra care must be used when applying some of these steps, since misapplication could harm the workstation configuration. Each installation and situation requires individualized attention.

14. Are there any issues with SPS and CITRIX?

Citrix has some known issues with multiple virtual USB Ports that are installed during the installation of Datakey IKey drivers. There are two ways to address the problem:

a) You can either change the Citrix configuration to not look for a Crypto Token on all of the virtual ports
b) You can change the iKey driver to be more acceptable to Citrix

Here is how to perform the above fixes:
a) Change the Citrix configuration to not look for a Crypto token:

1) Locate the MODULE.INI file in C:\Program Files\Citrix\icaweb32 directory
2) Open MODULE.INI file with notepad and go to [ICA 3.0] section
3) Look for "VirtualDriver =" entry
4) Remove the word "**Smartcard**" then save the file.
5) Restart the system.

b) Change the iKey driver to be more acceptable to Citrix: Modify the iKey driver installation to have only one virtual reader. Note that this approach allows only one iKey to be used on the system at any one time.

1) Uninstall the iKey driver using Add/Remove Programs.
2) Restart the system.
3) Install the iKey driver from the command prompt using the parameters shown below:
   ```
   ikeydrvr -a VR=ON READERS=1
   ```
4) Restart the system.

Questions and Answers - Public Key Infrastructure

15. What is the PKI (Public Key Infrastructure) used in SPS?

SPS uses a Fiscal Service PKI infrastructure hosted by Bureau of Public Debt in Parkersburg, West Virginia.

16. Can the SPS co-exist with other PKI applications?

Probably not. The current version of SPS is not capable of co-existing with other PKI credentials used by other applications. Future versions of SPS are expected to be more flexible that allows such co-existance.

17. Can SPS use/work with a different PKI?

No. The current version of SPS is not capable of working with a different PKI infrastructure. Future versions of SPS are expected to be more flexible that allows different PKI credentials that can be accessed through "Treasury Bridge."

18. Can SPS share credentials with other applications?

No. The current version of SPS is not capable of sharing PKI credentials with other applications. Future versions of SPS are expected to be more flexible that allows such sharing.

19. Can SPS use a different smart card/IKey?

No. SPS is designed specifically using SmartCard/IKeys from the DataKey vendor.

20. Why does SPS not use the secure port access (636) to LDAP?

LDAP is used to access PKI certificates and CRLs (Certificate Revocation Lists) which is all public information. Also, the PKI certificates and the CRL data is signed by CA (Certificate Authority) -- we validate the data first before using it.

Consequently, we are using "normal" LDAP port 389 instead of the "secure" LDAP port 636 to access information from LDAP.

Questions and Answers - Security

21. What kind of encryption is used in SPS? What kind of security is used in SPS?

SPS is designed to use multiple levels of encryption for all its communications. First, a secure, dual-authenticated SSL tunnel using “Triple DES” encryption is used to create a secure communication channel between end-user machines and the SPS web server. Next, every message sent through the SSL tunnel is encrypted using “AES 128” encryption using the Public Keys of the recipient. Finally, messages are signed using digital signatures to ensure integrity, authentication and to provide non-repudiation.

For more information on this topic, please refer to the document entitled “SPS Security Overview”.

22. Are there any issues with SPS and NIST security recommendations?

Not really, but the implementation of NIST security recommendations needs to be revisited to take into consideration the needs of SPS. Specifically, if the implementation of NIST security recommendations involves disabling of any unwanted services in the Microsoft Windows XP/2000 operating systems, the Smart

Card services may in the list of disabled services.   How ever, SPS needs Smart Card services for its cryptographic functions and hence should not be disabled.